

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-324484

(43)Date of publication of application : 07.12.1993

(51)Int.Cl.

G06F 12/14

(21)Application number : 04-127787

(71)Applicant : CSK CORP

(22)Date of filing : 20.05.1992

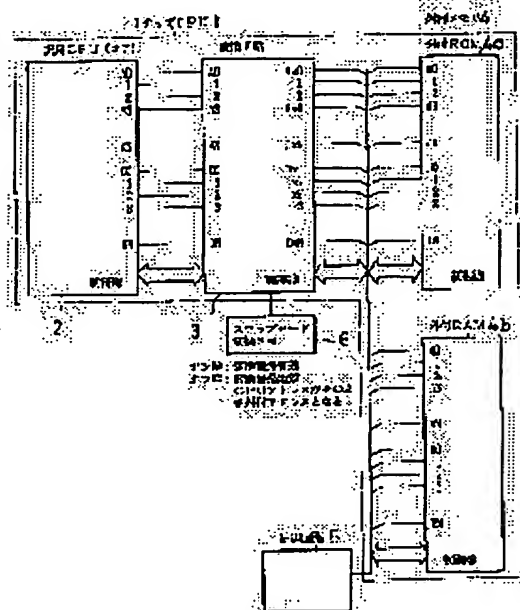
(72)Inventor : KAWAMURA TAKAYUKI

(54) SECURITY SYSTEM FOR EXTERNAL MEMORY

(57)Abstract:

PURPOSE: To improve privacy and safety by translating the addresses and bits of an external memory with a pattern decided the arrangement beforehand at random by a translating means between a general-purpose CPU (core) and the external memory.

CONSTITUTION: A one-chip CPU 1 is composed of a general-purpose CPU (core) 2 and a translation circuit 3, a ROM 4a and an external RAM 4b are additionally connected to an external memory 4 externally attached to the one-chip CPU 1, and the addresses on the side of the general-purpose CPU 2 are connected corresponding to the CPU side addresses and data of the translation circuit 3. Similarly, the translation circuit 3 and the external memory 4 are correspondently connected. When a swap mode changeover switch 6 for a peripheral circuit 5 and the translation circuit 3 is turned on, a translation table is made valid, when it is turned off, the table is made invalid, and the CPU side addresses are connected to the memory side additionally. In this case, the translation circuit 3 is composed of a SRAM, the contents of the translation table in the external memory are arbitrarily changed and composed of various translation patterns. Namely, it is difficult to analyze the contents of the external memory 4.



LEGAL STATUS

[Date of request for examination] 17.07.1996

[Date of sending the examiner's decision of rejection] 01.06.1999

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁(JP)

(12) 公開特許公報(A)

(11)特許出願公開番号

特開平5-324484

(43)公開日 平成5年(1993)12月7日

(51)IntCl⁵

G 0 6 F 12/14

識別記号

3 2 0 B

庁内整理番号

9293-5B

F I

技術表示箇所

審査請求 未請求 請求項の数1(全 8 頁)

(21)出願番号 特願平4-127787

(22)出願日 平成4年(1992)5月20日

(71)出願人 000131201

株式会社シーエスケイ

東京都新宿区西新宿2丁目6番1号

(72)発明者 川村 孝之

東京都新宿区西新宿2-6-1 株式会社

シーエスケイ内

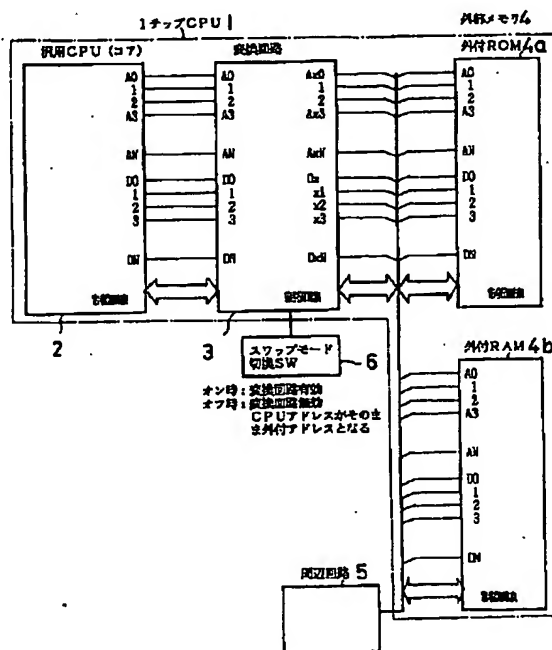
(74)代理人 弁理士 宇高 克己

(54)【発明の名称】 外部メモリのセキュリティシステム

(57)【要約】

【目的】 1チップCPUの外付けする外部メモリのセキュリティを高める為になされたものであり、第三者による外部メモリに格納されるデータの呼出し、変造を防止し、データの機密性、安全性を高めた外部メモリのセキュリティシステムを提供することである。

【構成】 汎用CPUと、この汎用CPUに外付けされた外部メモリを備えて構成された特定用途向けの1チップCPUにおける前記外部メモリのセキュリティシステムであって、前記汎用CPUと外部メモリ間に配置されると共に前記外部メモリに格納されているデータのアドレス及びデータ内容を示すビット配列の変換機能を有する変換手段を有した外部メモリのセキュリティシステム。



1

【特許請求の範囲】

【請求項1】 汎用CPUと、この汎用CPUに外付けされた外部メモリを備えて構成された特定用途向けの1チップCPUにおける前記外部メモリのセキュリティシステムであって、前記汎用CPUと外部メモリ間に配置されると共に前記外部メモリに格納されているデータのアドレス及びデータ内容を示すビット配列の変換機能を有する変換手段を有することを特徴とする外部メモリのセキュリティシステム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は、特定用途／ユーザ向けのいわゆるカスタマイズの1チップCPU（マイコンチップ）に外付けしてなる外部メモリ（例えば外部ROM及び／又はRAM）に対する第三者からのアクセス即ちメモリデータの変改造を防止し、メモリデータの機密性、安全性を高めた外部ROMのセキュリティシステムに関するものである。

【0002】

【従来の技術】 近年、マイコンチップを用いたコンピュータシステムにおいては、ASIC（特定用途向けIC）技術の革新により汎用CPUを中心にして特定用途向けに開発された回路を複数配して構成した特定用途／ユーザ向けのいわゆるカスタマイズされた1チップCPUが盛んに用いられている。そして、このカスタム（ASIC）1チップCPUは標準ICを使って構成されたものよりも部品点数が少なく済み、コストも安く、動作速度は速くなり、故障も少なくなる等有用な点を種々有していた。

【0003】 一方、1チップCPUに限らずチップに組み込まれるプログラムの規模（ステップ数で示される）が大きいシステムの場合にはプログラムエラーの発生確率も高くなり、しかもプログラムを長期間に渡って運用していく場合には必ず必要なプログラムの部分変更の際には1チップCPU自体を交換しなければならずコスト的にも問題があった。このような事情から、一般的には書換が可能な外部ROM（PROM、EPROM、EEPROM、フラッシュメモリ等）及び／又は外部RAMを1チップCPUに外付けして使用していた。そして、このような外部ROM及び／又は外部RAMはカスタム1チップCPUに一体的に接続されており、この外部ROM及び／又は外部RAMのデータ内容を比較的容易に解説することができるような構成即ち、外部ROM及び／又は外部RAMの内容が汎用CPUの命令系統を共有している構成をとっているために、第三者による恣意的なデータ変造等に対して無防備であり、データの秘匿性、安全性の低下といったセキュリティ上の問題が生じており何らかの解決策が求められていた。

【0004】

【発明が解決しようとする課題】 本発明は以上のような

2

問題点を解決するためのものであり、その目的は、1チップCPUの外付けする外部メモリのセキュリティを高める為になされたものであり、第三者による外部メモリに格納されるデータの呼出し、変造を防止し、データの機密性、安全性を高めた外部メモリのセキュリティシステムを提供することである。

【0005】

【発明の開示】 上記本発明の目的は、汎用CPUと、この汎用CPUに外付けされた外部メモリを備えて構成された特定用途向けの1チップCPU（ASIC技術にてゲートアレイ上に汎用CPUと変換手段で組み合わせた専用のチップ）における前記外部メモリのセキュリティシステムであって、前記汎用CPUと外部メモリ間に配置されると共に前記外部メモリに格納されているデータのアドレス及びデータ内容を示すビット配列の変換機能を有する変換手段を有することを特徴とする外部メモリのセキュリティシステムによって達成される。

【0006】

【作用】 即ち、外部メモリのセキュリティシステムにあつては上記の如く、外部メモリのデータ内容を直接司る汎用CPU（コア）とこの外部メモリとの間に交換手段を配置し、この交換手段によって外部メモリに格納されるデータのアドレス、ビットの配列を予め決められたパターンでかつ内容的にはランダムに変換することによって、外部メモリの内容を第三者に覗かれ、解析されそして変造されるのを防止できるものである。

【0007】 このようにデータ内容を覗かれたり、更には変造される虞は解消され、その結果、秘密データの秘匿化、セキュリティの確保が達成できる等総合的なデータやシステム管理が行なえる。即ち、従来のように外部メモリの内容が汎用CPU（コア）の命令体系である場合に容易にこの外部メモリにアクセス（リード／ライト）されてしまつてデータ内容を覗き見られたり、変造されたりするトラブルが解消されるものである。

【0008】

【実施例】 図1乃至図8は、本発明に係る外部メモリのセキュリティシステムの一実施例を示すもので、図1は本システムに用いられる1チップCPU及び外付メモリの接続態様の概略構成図、図2は同様にワイヤー結線で見えた場合の変換の概略を示した図、図3は1チップCPU内に用いられる変換回路のブロック構成図、図4は外部ROM上に格納されているメモリマップ構成図、図5は汎用CPU側から見た外部メモリ空間のメモリマップ構成図、図6は変換テーブル格納領域と変換回路との関係を示す説明図、図7は変換テーブルの使用例を示した説明図、図8は変換回路の内部結線の変換による外部ROM側のアドレスの変化を示す説明図、図9は外付ROMのプログラムの方法の説明図である。

【0009】 図1中、1はASIC技術にてゲートアレイ上に汎用CPUと変換手段とで構成される1チップC

PUであり、汎用CPU2と変換回路3とにより構成されている。4はこの1チップCPU1に外付される外部メモリであって、外付ROM4a、外付RAM4bが接続されている。そして、汎用CPU2側のアドレス(A0~AN)、データ(D0~DN)と変換回路3のCPU側のアドレス(A0~AN)、データ(D0~DN)とはそれぞれ対応して結線されている。同様に変換回路3の外付メモリ4側のアドレス(Ax0~AxN)、データ(Dx0~DxN)と外付メモリ4側のアドレス(Ax0~AxN)、データ(Dx0~DxN)とはそれぞれ対応して結線されている。5は周辺回路、6は変換回路のスワップモード切換スイッチであり、オン時には変換テーブルを有効とし、オフ時には変換テーブルを無効としてCPU側アドレスがそのまま外付メモリ側に接続されるものである。

【0010】以下に図3のブロック構成図に基づいてスワップモード切換スイッチ6がオン時の変換テーブル使用態様を説明する。31は変換テーブル格納アドレス発生用のカウンタ(CNT)である。32は汎用CPUに対してデータバス使用権利の放棄を要求するF/F(フリップフロップ)である。33はSRAM#1(スタックRAM)であり、アドレス変換ブロック(0~255ブロック)の中の1つのブロック(256バイト)単位内のアドレスを任意に決めるための変換テーブル格納用として用いられるものである。34は同様にSRAM#2(スタックRAM)であり、アドレス変換ブロック(0~255ブロック)ブロック番号を任意に決めるための変換テーブルの格納用として用いる。35、36はセクタ(SEL)であり、変換テーブル格納アドレス発生用カウンタ値とCPUから出力されるアドレスを切り換えるためのものである。37も同様にセクタ(SEL)であり、変換テーブル(SRAM#1(33)、SRAM#2(34))に書き込むデータを切り換えるためのものである。38はSRAM#1(33)、SRAM#2(34)のチップセレクト(CS)信号及び書き込み(WE)信号を発生させるデコーダである。

【0011】B1はCPU2から出力されるアドレスA0~A15(計16本)のアドレスバスである。(CPUのアドレス空間が64Kとした例を示す。尚このCPUのアドレス空間が広がればA15がA23というようにアドレス(バス)の数は対応して増加する。)B2はデータバスであり、CPU2側のデータバスに接続され、双方向データバスである。B3は外部データバスであり、外部メモリ4側のデータバスに接続され、双方向データバスである。B4は変換回路3から出力されるアドレス(Ax0~AxN)と外部メモリ4側アドレス(A0~A15)とを接続するアドレスバスである。そして、変換テーブル格納アドレス(FE00H~FFFFH)の読込みのために用いられる。即ち、CPU2から出力されるアドレスが(A0~A15)が変換テーブル(SRAM#1(33)、SRA

M#2(34)内のアドレス(Ax0~AxN)を経由して外部メモリ4側に出力されるものである。

【0012】S1はカウンタ(CNT)31をカウントアップするためのクロック信号(CLK。)である。S2はリセット(RESET)信号である。S3は変換回路3からCPU2に出力され、バス使用権利の放棄を要求する信号(CPUREQ)である。S4はCPU2から出力されるメモリリード要求(MEMRD)信号である。S5はSRAM#1(33)、SRAM#2(34)に書き込み要求信号を外部メモリリード要求(MRD)とした信号であり、変換テーブル格納データ内容読込のために用いられる。そして通常動作時、CPU2から出力されるメモリリード要求(MEMRD)信号S4とマルチプレクス(高速処理)された信号となっている。

【0013】以下、図3に基づいて1チップCPU1内の変換回路3の動作について説明する。即ち、変換回路3をSRAM(或いはEPROM)等で構成し、外部(汎用CPU2側からダウンロードして、汎用CPU2と外部メモリ4のアドレス(A0~A15)及びデータ(D0~DN)とを任意(ランダム)な結線とする場合を例にとって説明する。尚、データ(D0~DN)を変換する場合にはSRAM#1(33)、SRAM#2(34)と同様の交換RAMを設ける。(概略的には図2に示す如く構成するものである)尚、前提条件としてのメモリ空間の構成を図4のアドレスマップについて説明する。又、CPU2のアドレス空間が広がれば変換テーブルのアドレスも同様に變更される。同様に変換回路内のCNT31も變更されるものである。

① 汎用CPU2側のアドレス空間は64Kバイトであり、データ長は8ビットとする。

② アドレス変換テーブルは256バイト×2=512バイトとする

③ アドレス変換テーブルは番地FE00~FFFFに格納するものとする。

④ SRAM#1(33)、SRAM#2(34)と、デコーダ38、セクタ35、36、37にはそれぞれデータの移動・演算速度が高速(データ遅延量が少なく済む)である部品が使われている。即ち、CPUが本来有している最大アクセススピードを損なうことなく命令及びデータのリード/ライト動作を最小限にして実行させるためである。なぜならば外部データバスB3、外部アドレスバスB4により接続される外付ROM4a、外付RAM4b等にアクセスする時にはいわゆるウエイト機能を挿入しなければならないものである。尚、このウエイト機能とは外部アドレスをデコードしてCPU2に対するウエイト(待機)信号を送出する機能あるいはCPU2内にウエイト(待機)制御用のレジスタを設定可能であるならば、設定したレジスタによってウエイト(待機)時間を適宜に設定する機能を有するものであ

る。

【0014】以上のような前提条件下において、

(1) パワーオン(或いはリセット入力後)、カウンタ31及びF/F32はリセット状態となる。

(2) リセット信号S2の入力により、F/F32はクリアされ、CPU2に対してCPUREQ信号S3(バス使用権限の放棄を要求する信号のアクティブ“L”)を送出する。この信号の出力でもってCPU2はCPUREQ信号S3の“H”が入力するまでバス使用権限を放棄した状態が保持されるものである。

(3) カウンタ31から変換テーブル格納番地(FE00H)が外部メモリ4のアドレスに出力される。そして、下位8ビットはセクタ35を経て、SRAM#1(33)、SRAM#2(34)に対するアドレスとなる。同時にデコーダ38からSRAM33のチップセレクト信号(CS)と書込み信号(WE)が出力される。この時の書込み信号(WE)は外部メモリ4に対する外部メモリリード要求信号S5となる。この場合、セクタ35、36、37はAサイド側が有効状態となる。

(4) カウンタ31から出力された変換テーブル格納番地はセクタ36を経て外付ROMに出力される。アドレスの指定並びに外部メモリリード要求信号S5の送出により外部メモリ4からデータが1バイト読み込まれ、そのデータがセクタ37のAサイドからSRAM#1(33)に書き込まれる。

(5) これ以後、カウンタ31により外部メモリ4に対するアドレスが“1”だけプラスされ、このアドレスがFEFFH(256バイト)に達するまで前記(1)～

(3)を繰り返す。即ち、外部メモリ4のアドレス(FE00H～FEFFH)がSRAM#1(33)のアドレス(00H～FFH)に書き込(コピー)まれる。尚、SRAM#1(33)のソフト内容としての変換テーブルは全メモリ空間を構成する256ブロックの内の1ブロック内のアドレスを決定するために用いられるものである。(図4及び図7参照)

(6) カウンタ31がアドレス(FF00H)になった時にSRAM#2(34)が選択され(デコーダ38によってSRAM#2(34)を選択する信号が出力される)、外部メモリ4のアドレス(FF00H～FFFFH、256バイト)までの内容がSRAM#2(34)に書き込(コピー)まれる。即ち、外部メモリ4のアドレス(FF00H～FFFFH)がSRAM#2(34)のアドレス(00H～FFH)にコピーされるものである。尚、SRAM#2(34)のソフト内容としての変換テーブルは全メモリ空間を構成する256ブロックの内の1つのブロックのブロック番号を決定するために用いられるものである。(図4及び図7参照)

(7) 外部メモリ4のアドレス(FE00H～FEFFH、256バイト)をSRAM#1(33)にアドレス(FF00H～FFFFH、256バイト)をSRAM#2(34)に全

て書き込んだ後、カウンタ31からキャリー信号(CY)が出力され、F/F32の出力即ちCPUREQ信号S3の出力が“H”となり、CPU2はバス使用権限を獲得するものである。この時、セクタ35、36のBサイド側が有効となりセクタ37は使用禁止状態となり、SRAM#1(33)、SRAM#2(34)のチップCS(チップセレクト信号)は常に有効、WE(書込み)は常に禁止状態となる。

(8) この状態で、CPU2は通常動作であるアドレス0番地(0H)からスタート可能状態(スタンバイ)となる。

(9) 図8にイメージ的(概略的)に示されるように、この状態でCPU2は0番地(0H)をアクセスするが、実際にはSRAM#1(33)、SRAM#2(34)によりアドレス変換されており、機械的に外部メモリ4のアドレス番地をアクセスするのではなく、変換テーブルの変更に従ったアドレスがアクセスされることになる。そして、CPU2と外部メモリ4のそれぞれのアドレスを任意(ランダム)に結線する内容の変換テーブル格納する外部メモリ4の(FE00H～FEFFH、256バイト)のデータ内容は256バイト内の配置を任意に変換させることが目的であるので同じ値が書き込まれることはない。(もしくは禁止事項とする)尚、上記説明ではSRAMを2つ用いた内容で説明してきたが、その他のバリエーションとしてSRAMを更に増やしたり、あるいはアドレス(A0～AN)、(Ax0～AxN)とデータ(D0～DN)、(Dx0～DxN)との組合せについておこなえば、より複雑なパターンで暗号化が達成できる。

【0015】更に、ROM化する上でのアドレス変換の行い方について図3並びに図9を用いて説明する。即ち、

(1) 変更前(通常のROM内容)

物理アドレス=論理アドレス

(2) 変更後(アドレスビットを入れ換えた時のROM内容)

変更前の論理アドレスが図8のように配置されており、従ってこのROMにプログラムを書き込む場合には論理アドレスに配置換えした形に変更する必要がある。

【0016】以上説明してきたように、変換回路3をSRAM(もしくはE²PROM)で構成することにより外部メモリ4上の変換テーブル(SRAM#1(33)、SRAM#2(34)に対応する)の内容をそれぞれに任意に変更することができるので種々の変換パターンでもって構成するので、即ち具体的にはアドレス及びデータのビット配列をランダムに暗号化(インターリーブを含む)されたことになり、外部メモリ4内に格納される内容(プログラム)の第三者によるデータの解析は非常に困難なものとなり、事実上不可能といっても良く、従って破壊や詐取といった甚大な被害を事前に防止することができ、その結果、秘密データの秘匿化、セ

セキュリティの確保が達成できる等総合的なデータ及びシステムの管理が達成できる。

【0017】

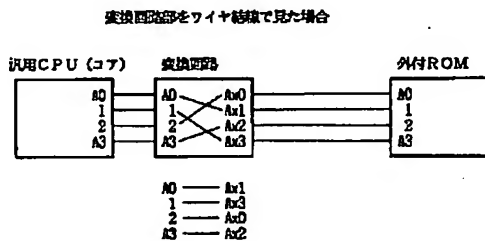
【効果】本発明に係る外部メモリのセキュリティシステムは、外部メモリのデータ内容を直接司る汎用CPU（コア）とこの外部メモリとの間に配置した変換手段によって外部メモリに格納されるデータのアドレス、ビットの配列を予め決められたパターンでかつ内容的にはランダムに変換させておくので、いわば、暗号化が成され、外部メモリの内容を第三者に覗かれ、解析されそして変造される虞は解消され、その結果、秘密データの秘匿化、セキュリティの確保が達成できる等総合的なデータやシステム管理が行なえる。

【0018】即ち、従来のように外部メモリの内容が汎用CPU（コア）の命令体系である場合に容易にこの外部メモリにアクセス（リード/ライト）されてしまつてデータ内容を詐取されたり、変造、破壊されることが無くなるものである。

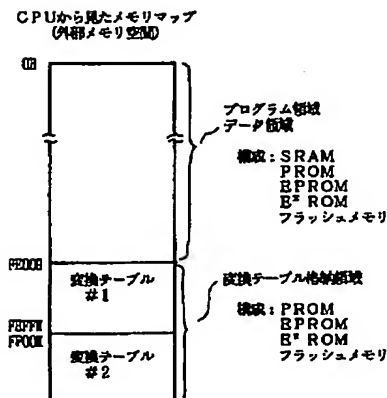
【図面の簡単な説明】

【図1】本システムの1チップCPU（ASIC技術によりゲートアレイ上に汎用CPUと変換回路と組み合わせたもの）と外付メモリの接続態様の概略構成図である*

【図2】



【図5】



* 。

【図2】本システムにおいてワイヤ結線で見した場合の変換の概略を示した図である。

【図3】本システムの1チップCPU内に用いられる変換回路のブロック構成図である。

【図4】本システムの外部メモリ上に格納されているメモリマップ構成図である。

【図5】本システムの汎用CPU側から見た外部メモリ空間のメモリマップ構成図である。

10 【図6】本システムの変換テーブル格納領域と変換回路との関係を示す説明図である。

【図7】本システムの変換テーブルの使用例を示した説明図である。

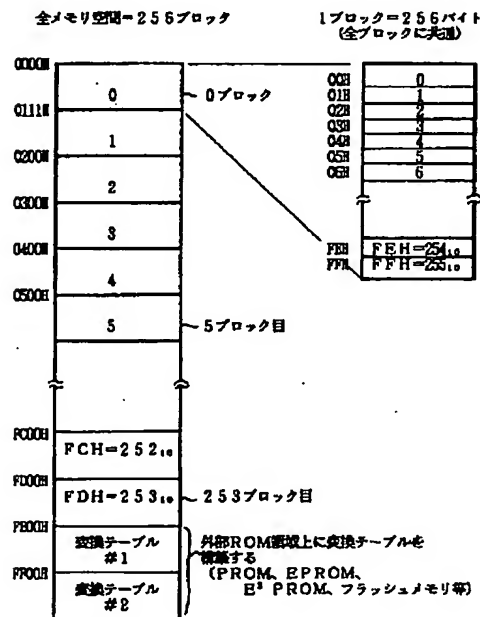
【図8】本システムの変換回路の内部結線の変換による外部ROM側のアドレスの変化を示す説明図である。

【図9】本システムの外付ROMのプログラムの方法の説明図である。

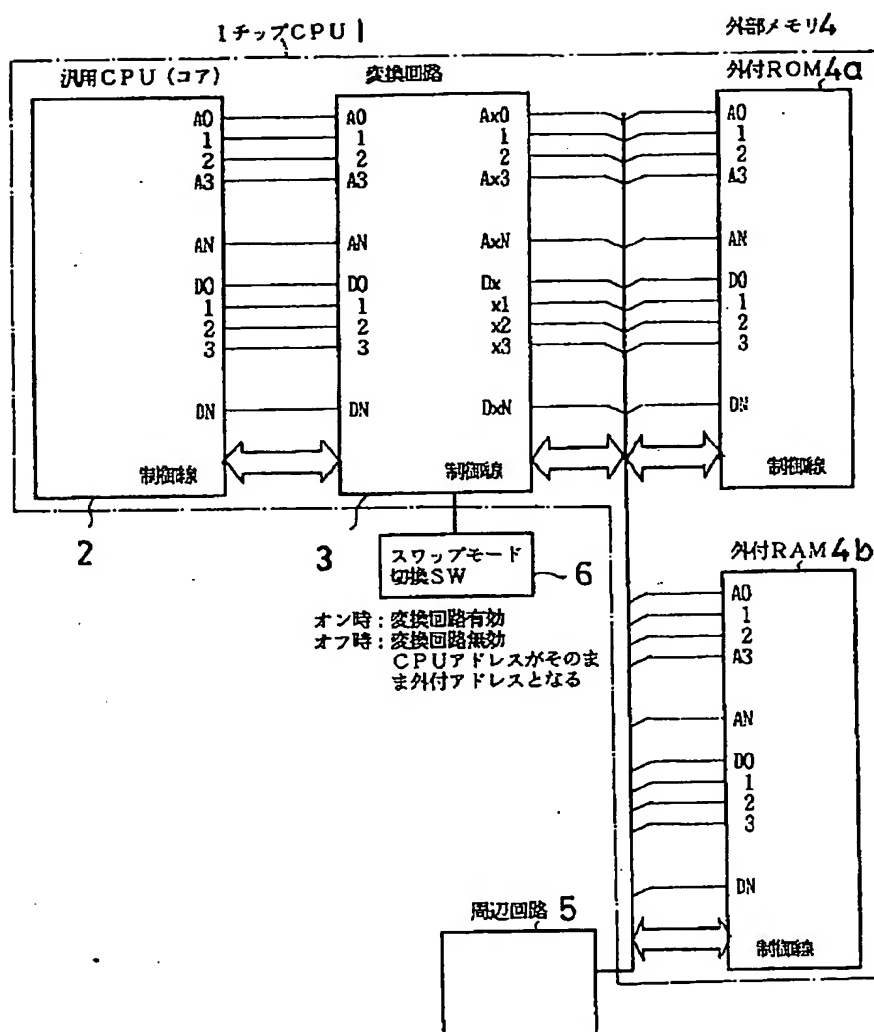
【符号の説明】

- 1 1チップCPU
- 2 CPU
- 3 変換回路
- 4 外部メモリ

【図4】

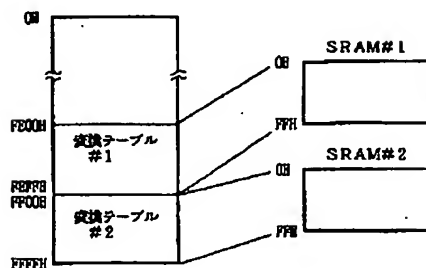


【圖 1】

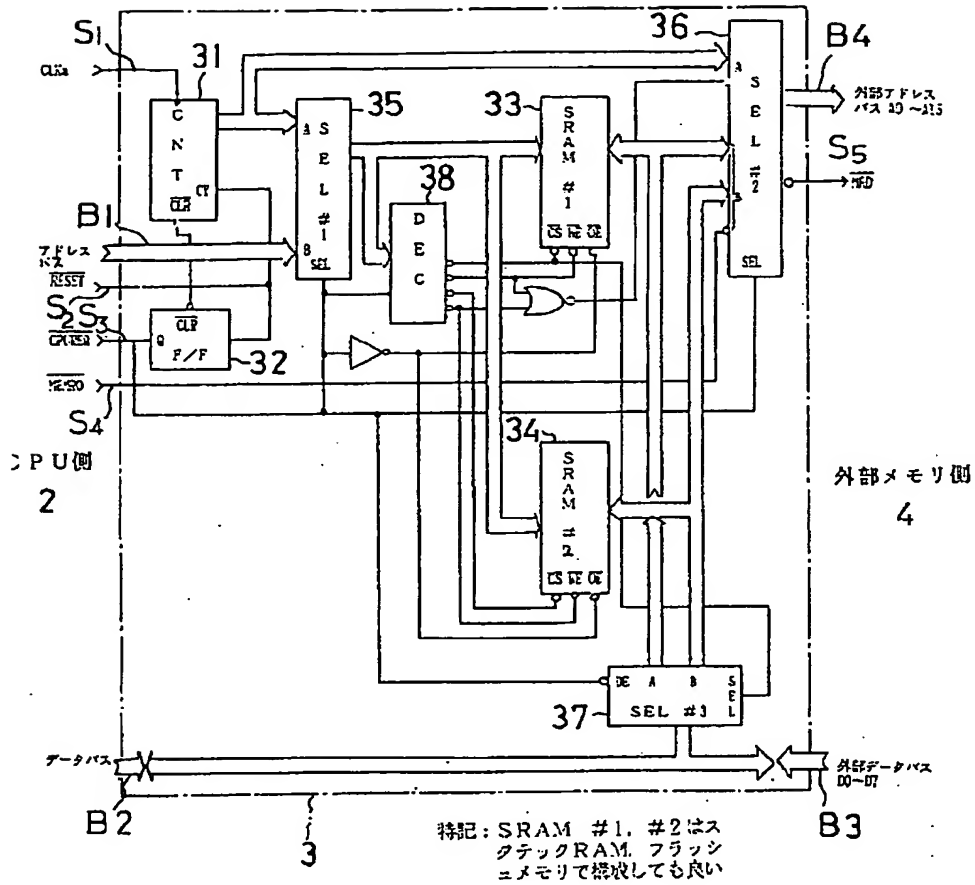


【圖 6】

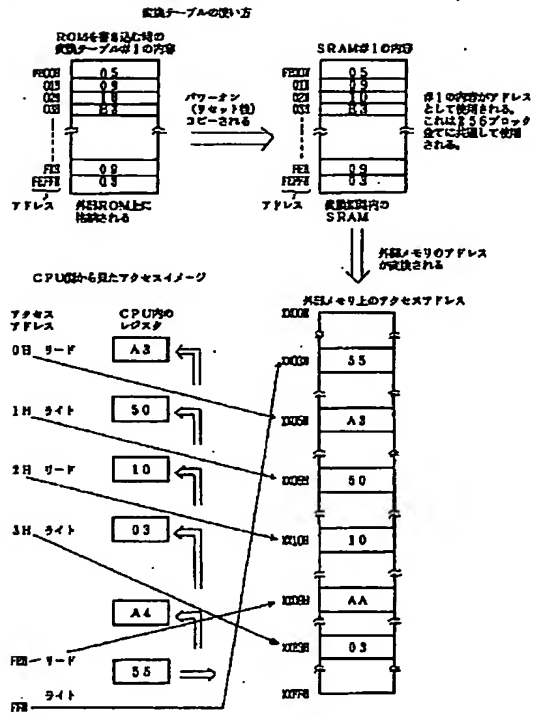
変換テーブル格納領域と変換回路 (SRAM#1、#2) との関係



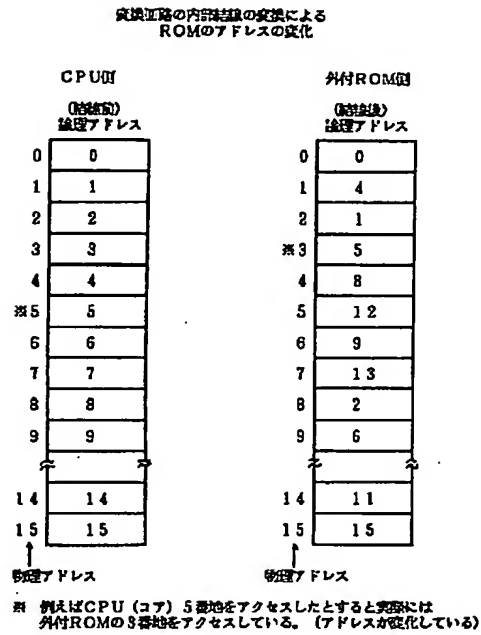
【図3】



【図7】



【図8】



【図9】

